Federal Computer Incident Response Capability

The FedCIRC Bits & Bytes

A monthly newsletter for Information System Security Managers/Officers & System Administrators

August 1, 2000 Volume I, Issue 2

A Note from the Director

Use of the Internet Can Open Many New Windows

but maybe consideration should be given to closing a few of them. Every day, incident reports are filed with FedCIRC detailing an altered web site, root compromised host or other malicious activities that could have been prevented. The cause — Exploitation of a commonly know weakness in an operating system or application for which corrective patches or configuration fixes are widely publicized.

The real problem is not the vulnerability introduced by the weakness but lack of attention to bulletins, vulnerability alerts and directions on how to correct the flaws. At FedCIRC, we see far too many reoccurrences of defaced web sites where the perpetrator exploits the same vulnerability over and over again. Responsible network management requires attention to details and the implementation of available security patches. Additionally, active but unnecessary ports on network hosts continue be a significant vulnerability and contribute to the mounting number of compromises occurring every day. Any port service (SMTP, FTP, TELNET, etc.) that is not mission essential should be closed to prevent an intruder from gaining access to critical services or information. Those ports and services required only by internal staff should be blocked at the router or firewall to prevent external use.

You wouldn't hand a stranger the keys to your house so why give a would-be intruder the keys to your network. Secure those unnecessary windows to the cyber-world and install patches as they are made available. Your boss will appreciate it.

Director,

Validating the Patches for the Patch Dissemination Process

In the July edition of FedCIRC Bits and Bytes, we provided an overview of the process for disseminating validated patches that FedCIRC is developing. Now, we are going to provide a glimpse of how we are going to validate the various patches. The operating systems (OS) for which the patches will be validated will be the major Microsoft Windows OSs, such as Windows 2000, Windows NT 4.0, and Windows 98. We will also look at several versions of Novell NetWare and the various commercial versions of UNIX, as well as open source OSs such as Linux and BSD. We will also look at the major applications that run on these OSs.

FedCIRC will establish a test lab where we will validate the patches. The patches will be obtained from their official source, whether it is a commercial site, a government site, or the open source maintenance site for each OS or application. The documentation that comes with the patch code will be reviewed and validated along with the patch source code to ensure that there are no back doors or confusing statements in either. If questions arise, they will be answered by working with the appropriate author. The patches will also be tested to see what side effects their implementation will have on other software applications.

Once the patch has been validated, it will be placed on the Secure Patch Dissemination Server. The downloadable package will include the patch, documentation, a validation report that will include any minor occurences, detected side effects, and a suggested secure configuration.

Windows of Insecurity

by: NIST (ITL Bulletin, 6/2000)

Even the best security technology, policies, and procedures do not guarantee the security of a system. As seen with the Hotmail bug, a presumably secure system can become completely insecure overnight if a perpetrator discovers a bug and posts an exploit on the Internet. People should certainly configure their systems correctly, install all patches, use firewalls, deploy an intrusion detection system, routinely review system logs, and regularly update their virus checkers. However, these techniques typically only prevent and detect known attack methods. If an attacker uses a new attack while engaging in a legitimate conversation with a system, the attack will go undetected and unstopped by the aforementioned methods.

About 30-40 unique computer attacks are published monthly on the Internet. For a certain amount of time after each attack is published, attackers have free rein to break into networks because administrators have not yet been able to apply a workaround or patch. It often takes incident response organizations hours to release workarounds and days to release patches. When that time is added to the time it takes an administrator to become aware of the problem and apply the patch, attackers have a large window of opportunity with every attack that is published. Since new vulnerabilities are discovered on a daily basis, patient attackers can wait for an applicable vulnerability to be published before launching an attack against their desired target.

System Administrators should check websites such as the www.fedcirc.gov, www.microsoft.com/technet/security/current.asp, and www.cert.org on a regular basis for more information.

Viruses, Worms, & Trojans in the Wild

PICA: Also known as *I-Worm.Lee*

VBS.Jer(htm): Also known as *JER.HTM, VBS.1ON1MAIL, VBS.Jer, VBS_Jer*

VBS/COD: Also known as *Crayon of Doom, LIST.VBS, PORNLIST.DOC*

Viruses, Worms & Trojans continued....

VBS.Plan: Also known as *VBS.Loveletter.AS, I-Worm.Plan*

Major Anti-Virus vendors have posted information on the above listed viruses/worms/trogans and provide software to detect and prevent infection by many other variants of the LoveLetter worm.

Executive and Legislative Watch

The recent cyber-attacks against government and private sector Internet sites have raised awareness for the need to increase cyber-security to protect the nations assets. Whether they came from a domestic perpetrator, terrorist group or hostile nation, these attacks can cause significant damage to the nations critical infrastructure. The following are initiatives taken by the Executive branch and Congress to address cyber-security:

National Plan for Information Systems Protection- Establishes the mechanisms for the protection of critical infrastructures from attack.

HR 4246 – Encourages the secure disclosure and protected exchange of information about cyber security problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection.

H Con. Resolution 285 – Designates cyber-terrorism as an emerging threat to the national security of the United States and the nation's electronic infrastructure. Calls for: a partnership between the Federal government and private industry in combating the cyber menace; a revised legal framework for prosecution of hackers and cyber-terrorists; and a new interagency study to assess the threat posed by cyber-terrorists.

S 2448 Internet integrity and Critical Infrastructure Protection Act of 2000 - Enhances the protection of the Internet and the critical infrastructure of the United States.

S 2092 modifies the Electronics Communications Privacy Act of 1986 – Allows for effective investigation and prosecution of cyber-crimes. Would allow for a single court order to completely trace a computer attack from the victim back to the attacker.

S 1993 Government Information Security Act – Reforms government information security by strengthening information security practices throughout the Federal government.

Calendar of Events

FedCIRC Partners Meeting
Date: Aug 17, Oct 19, Dec 14, 2000 @ 9:00am
Location: GSA NCR Bldg, Room 5700, Washington, DC
POC: 202-708-5060
http://www.fedcirc.gov

Computer Security Incident Handling for Technical Staff (Introductory)
Date: Aug 21-25, 2000
Location: Carnegie Mellon Univ, Software Engineering Institute (CERT/CC), Arlington, VA
POC: 412-268-7702
http://www.sei.cmu.edu/products/courses/security-incident.html

Managing Computer Security Incident Response Teams (CSIRTs)
Date: Sept 12-14 or Nov 14-16, 2000
Location: Carnegie Mellon Univ, Software Engineering Institute (CERT/CC), Arlington, VA
POC: 412-268-7702
http://www.sei.cmu.edu/products/courses/managing-csirts.html

Computer Security Incident Handling for Technical Staff (Advanced)
Date: Oct 16-20, 2000
Location: Carnegie Mellon Univ, Software Engineering Institute (CERT/CC), Pittsburgh, PA
POC: 412-268-7702
http://www.cmu.edu/products/courses/csih-advanced.html

Introduction to Computer and Network Security
Date: Oct 31- Nov 1 or Nov 11-12, 2000
Location: varies
POC: Computer Security Institute, 415-905-2626
http://www.gocsi.com/wkshop.shtml

How to Become an Effective Information Security Professional
Date: Sept 20-21, 2000
Location: San Antonio, TX
POC: Computer Security Institute, 415-905-2626
http://www.gocsi.com/wkshop.shtml

Latest FedCIRC Advisories

FedCIRC Advisory FA-2000-13
Two Input Validation Problems In FTPD

Free Training Opportunities

F-Secure Corporation is collaborating with GartnerGroup to present a series of web-based briefings on Enterprise Security focused on wireless connectivity. The seminars are offered free of charge on a monthly basis through December 2000. The list of seminars are as follows:

- √ Security Issues for the Road Warrior
- √ Security Issues in Outsourcing with ASPs and ISPs
- √ End to End Security Issues for the Enterprise
- √ Security Issues for Wireless Devices
- √ Security Issues in Central, Policy Based Security
- √ A Blue Print for Enterprise Security

For more information: http://www.f-secure.com/securityonline/

The FedCIRC Bits & Bytes Newsletter

Director
David Jarrell
Project Manager for Marketing/Outreach
Connie Oden
Editor
Judy Dunsworth
Contributing Editors
David Adler
Kenneth Grossman

We welcome your input! To submit your related articles and notices for future issues, please contact FedCIRC at 202-708-5060. Deadline for submissions is the 15th of each month. Articles may be edited for length and content.